한눈에 보기

Cisco FirePOWER REST API

이점

- **액세스 및 관리:** 모든 Cisco FirePOWER 방화벽 정책 및 정책 구성 요소 지원
- **쉬운 내보내기:** Cisco FirePOWER 정책
- **읽기/쓰기 액세스:** Cisco FirePOWER Management Center의 주요 정책 및 관리 구성 요소에 대한 읽기/쓰기 액세스
- **API의 경량 및 유연한 작업 사용:** 보안 관리 및 위험 모델링 애플리케이션 지원
- **Cisco FirePOWER 구축 관리:** 다양한 방화벽 기술이 사용되는 구축 지원
- **세분화된 정책 관리 허용:** 외부 애플리케이션별 관리 가능

서드파티 플랫폼에서 Cisco FirePOWER 정책 관리

기업은 보통 수십 개의 보안 기술을 동시에 사용합니다. 이러한 보안 기술에는 다양한 소스에서 보안 상태 정보와 정책을 수집하는 툴이 포함됩니다. Cisco Firepower™ REST API를 통해 다양한 애플리케이션이 Cisco Firepower Management Center 플랫폼 및 연결된 Cisco Firepower 디바이스에서 정책, 주요 정책 요소 및 객체에 액세스하고 이를 분석할 수 있습니다.

REST API는 AlgoSec, FireMon, Skybox 및 Tufin 등의 벤더를 통해 독점 관리 플랫폼이나 FPM(Firewall Policy Management) 및 NSPM(Network Security Policy Management) 솔루션을 사용하는 고객에게 매우 유용한 툴입니다. FPM, NSPM 및 유사 기술에서 API의 읽기 및 쓰기 기능을 사용하여 관리 기능을 폭넓게 수행할 수 있습니다. 이러한 관리 기능의 범위는 완벽한 정책 마이그레이션에서 감사 기록, 디바이스 및 그룹 정보, 물리적 인터페이스 및 가상 스위치 등 Cisco Firepower의 특정 요소와의 연계에 이르기까지 다양합니다.

Cisco FirePOWER 기술의 확장성 및 외부 관리 애플리케이션으로 작업할 수 있는 기능으로 여러 방화벽을 동시에 실행하는 고객에게 편리함을 제공합니다. 또한 이전 기술에서 Cisco FirePOWER로의 전환이 더욱 쉬워졌습니다.

효율성 및 보안 모두 개선

차세대 방화벽 정책은 단일 REST API를 통한 외부 관리 및 위험 모델링이 가능합니다. Cisco FirePOWER 고객에게 서비스를 제공하는 MSSP(Managed Security Service Provider)는 API를 사용하여 대규모 다중 테넌트 인프라의 효율성을 높일 수 있습니다. MSSP는 고객 전반의 정책 업데이트를 손쉽게 수행할 수 있습니다.

최종 고객의 경우 이러한 효율성으로 보안을 대폭 강화할 수 있습니다. 최종 고객은 해커의 침입은 줄이면서 Cisco FirePOWER 차세대 방화벽에서 운용하는 최신 정책을 훨씬 더 빠르게 이용할 수 있습니다.

다음 단계

Cisco FirePOWER REST API에 대한 자세한 내용은 https://developer.cisco.com/site/firepower/를 참조하십시오.

Cisco FirePOWER API 및 기타 CSTA(Cisco Security Technical Alliance) 파트너 통합 및 이점을 활용하는 전략적 파트너에 대한 자세한 내용은 http://www.cisco.com/c/en/us/products/security/partner-ecosystem.html를 참조하십시오.

C45-737301-00 06/16